공격 트리를 이용한 산업 제어 시스템 보안 위험 분석

김경아* · 이대성** · 김귀남***

요 약

산업 현장에서 일반 컴퓨터와 윈도우 운영체계를 사용하여 생산 시스템을 제어 하게 되면서, 산업 시설에 대한 사이버 보안 위협이 심각한 문제로 대두 되고 있다. 네트워크와 연결된 산업 제어 시스템은 우리가 일상적으로 사용하는 PC나 기업의 정보 시스템에서 문제시 되던 악성코드의 공격에 노출되었다. 특히 컴퓨터 웜인 스턱스넷은 가스 수송관이나 발전소 같은 특정 산업 제어 시스템을 표적으로 하며, 이론상 물리적 타격도 가능하다. 본 논문에서는 산업 제어 시스템 구성 요소와 SCADA의 사이버 보안 위협을 살펴본 후, SCADA 보안 취약점을 조기에 파악하고 평가하여 가능한 사이버 공격을 사전에 대처할 수 있는 위험 분석 방법으로 공격 트리 분석을 고찰한다.

ICS Security Risk Analysis Using Attack Tree

Kim Kyung Ah* · Lee Dae Sung** · Kim Kui Nam***

ABSTRACT

There is increasing use of common commercial operation system and standard PCs to control industrial production systems, and cyber security threat for industrial facilities have emerged as a serious problem. Now these network connected ICS(Industrial Control Systems) stand vulnerable to the same threats that the enterprise information systems have faced and they are exposed to malicious attacks. In particular Stuxnet is a computer worm targeting a specific industrial control system, such as a gas pipeline or power plant and in theory, being able to cause physical damage. In this paper we present an overview of the general configuration and cyber security threats of a SCADA and investigate the attack tree analysis to identify and assess security vulnerabilities in SCADA for the purpose of response to cyber attacks in advance.

Key words : ICS, SCADA, Vulnerability, Attack Tree, Stuxnet, Cyber Security

접수일(2011년 12월 05일), 수정일(1차: 2011년 12월 13일), 게재확정일(2011년 12월 19일)

* 경기대학교 산업보안학과
** 경기대학교 산업기술보호특화센터
*** 경기대학교 융합보안학과

1. 서 론

정보 통신 기술의 발달로 인간-기기-네트워크의 연결이 폭발적으로 증가하면서 사이버 보안 위협도 기하급수적으로 늘어나고 있다.

전 세계 36개국 3300개 기업들을 대상으로 조사한 보안 현황 보고서에 따르면 가장 큰 비즈니스 위험 요소는 자연 재해나 테러가 아닌 사이버 공격이며, 기업들 중 71%는 사이버 공격을 경험했고, 21%는 정규적으로 공격을 받는 것으로 나타났다 [2].

기존의 폐쇄 직렬망인 ICS(Industrial Control Systems)도 TCP/IP와 Ethernet 같은 표준 프로토콜을 사용하여 제어 및 상태 감시를 위해 네트워크에 연결된 HMI(Human Machine Interfaces)를 가지게 되면서, 주로 기업의 정보 시스템에서 문제가 되어 왔던 보안 위협에 노출되어 사이버 공격의 표적이 되고 있다. 지난 한해 표적 공격은 질적으로 더욱 정교해 지고 양적인 규모도 확대 되었으며 방법도 다양해 졌다. SNS (Social Networking Service) 사이트에 내부 직원이 게시한 정보는 표적 공격의 일환으로 사회 공학적(social engineering) 공격 기법에 이용될 수 있으며, 또한 SNS는 사회 공학적 기법을 통해 악성 코드를 전파하는 플랫폼으로 악용되고 있다 [3].

스턱스넷(Stuxnet)은 최초로 산업 제어 시스템을 겨냥한 복잡하고 방대한 악성코드 일종으로 지멘스 SCADA(Supervised Control and Data Acquisition) 시스템인 Step7의 PLC 코드 변경이 목표이며 장기적인 공격을 전제로 보안 시스템을 우회하도록 설계되어 있다. SCAD는 주로 원자력 발전소, 생산자동화, 석유 및 가스 탐사, 그리고 유틸리티 감시 및 제어 등의 주로 핵심 인프라에 많이 사용되는 자동 제어 및 감시 시스템이다. 이란 부셰르 핵 시설에 대한 공격 사례를 통해 스터스넷은 서비스 거부(DDoS)나 스파이 활동을 하는 오로라(Aurora)와는 다른 차원으로 이론상 물리적 타격도 가능한 것으로 드러났다 [4][5].

주로 사후 배포된 보안 패치나 시그니처(signature) 기반의 바이러스 백신을 이용한 기업의 정보 시스템 보안과는 달리, ICS 보안은 사후 돌이킬 수 없는 결과를 초래할 수 있기 때문에 사전예방이 필수적 이다. 시스템의 잠재적 보안 취약성을 파악하고 위험 정도에 따라 그들을 구분하여 공격가능성을 사전에 차단하기 위한 방법으로 '위험 분석'이 있다.

본 논문에서는 공격 트리를 이용한 ICS 보안 위험 분석 방법을 고찰한다. 논문의 구성은 다음과 같다. 2장에서는 산업 제어 시스템 SCADA의 구조와 취약점을 살펴본다. 3장에서는 공격 트리 모델링 및 보안 위험 평가 방법을 소개한다. 4장에서는 스틱스넷의 공격 트리를 예로 제시한다. 5장에서 결론 및 향후 연구 방향을 밝힌다.

2. ICS 구조와 취약점

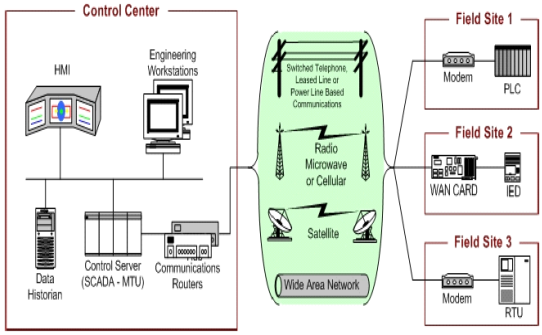
ICS는 SCADA, DCS(Distributed Control System), PLC(Programmable Logic Controllers) 등의 크고 작은 제어 시스템들로 구성되어 있다. ICSs는 전기, 물, 석유와 가스, 교통, 화학, 등의 산업에 사용되며, 고도로 연동된 상호 의존 시스템인 핵심 인프라 가동에도 필수적으로 자주 쓰인다. SCADA 시스템은 중앙집중식 데이터 수집 및 감독 컨트롤을 사용하여 분산된 자산을 제어하고, DCSs는 감독 및 규제 컨트롤을 사용하는 공장과 같은 로컬 영역 에서 생산 시스템을 제어하는데 사용되며, PLCs는 특정 애플리케이션을 위한 독립된 장치의 제어에 사용되어 일반적인 규제 컨트롤을 제공 한다 [6].

2.1 SCADA 시스템의 구성요소

아래 그림 1은 SCADA의 구성요소와 일반적인 배치도이다. 제어센터는 제어서버(SCADA Server 또는 Master Terminal Unit, MTU)와 통신 라우터, HMI, Engineering Workstations, 그리고 처리된 정보를 기록하는 데이터베이스(Data Historian)로 구성되어 있으며, 이들은 모두 LAN에 연결되어 있다. 제어 센터는 필드사이트에 의해 수집된 정보를 모아 기록하며, HMI에 정보를 표시하고, 감지된 이벤트에 따라 동작을 생성한다. MTU가 SCADA 시스템의 주 장치라면 원격 필드 사이트에서 데이터를 수집하고 제어하는 RTU(Remote Telemetry/Terminal Unit)와 부품의 논리기능을 수행하는 PLC는 종속장치로 작동한다. 필드 사이트의 IED(Intelligent Electronic Devices)는 로컬

수준의 자동 제어를 가능케 하는 스마트 센서/액추에이터(Actuator)이다.

제어 센터는 중앙 경보, 경향 분석 및 보고를 담당하고, 필드 사이트는 액추에이터에 대한 로컬 제어 및 센서 모니터링을 수행한다. 필드 사이트는 원격 액세스 기능을 갖추고 있어 필드 운영자가 공중 전화망(Dial-up) 또는 WAN 연결을 통해 원격 진단 및 복구를 수행할 수 있도록 한다. 직렬 통신을 통해 실행되는 표준 및 독자적 통신 프로토콜은 제어 센터와 필드 사이트 간에 정보를 전송하는 데 사용된다.



(그림 1) SCADA 시스템 구성 [6]

2.2 SCADA 시스템의 보안 취약점

제어 시스템은 원래 폐쇄망 형태의 구축/운영을 전제로 사이버 보안을 전혀 고려하지 않고 설계되었기 때문에 다양한 소프트웨어 취약점이 존재하며, 시스템 특성상 리부팅을 허용하지 않아 업데이트와 보안 설정 활성화에 한계가 있고, 독자적인 프로토콜 형식과 변형된 장비, 임베디드 운영체계로 인해 최적화된 보안 솔루션이 미비하다. SCADA 시스템의 취약점은 다음과 같다 [1][7].

- **조직의 불충분한 보안 정책: 보안 규칙을 정하고 집행하는 관리 메커니즘의 결여:** 보안 규칙에 대한 실행, 업데이트 또는 정규적 검토 결여, 내부 직원의 보안 인식 및 유지보수에 대한 보안 교육 부재
- **네트워크의 심층방어(defense-in-depth) 미흡:** SCADA의 핵심 제어장비인 PLC, RTU 또는 DCS에 대한 계층화된 보안 부족
- **부적합한 원격 접근 및 접근 기록 분실:** 접근 권한 분리 체계 미흡, 미인가 디바이스의 차단 관리/설정 부재, 부실한 로그 파일 관리
- **C&C(Command and Control)에 비전용 통신 경로 이용**: 인터넷과 연결된 SCADA 관리 및 모니터링 시스템
- **제어 시스템 PC와 무관한 소프트웨어 설치**: 미디어 플레이어, 게임 등 시스템 충돌 및 오작동 가능이 있는 베타 버전 소프트웨어 설치
- **제어 소프트웨어의 초기 테스트 부족:** 제어 소프트웨어에 대한 보안 준수 및 취약성 검증 부족

이 같은 SCADA 보안 문제 해결을 위해 보안 정책과 DMZ을 포함한 다층 아키텍처가 제안되었으며 [1][6], 잠재적 취약점에 대한 구체적인 파악과 체계적인 대응책을 마련하기 위해 공격 트리가 이용 된다 [11].

3. 공격 트리 모델링 및 평가

공격 트리의 개념은 공격자의 최종 행위 결과로부터 출발하여 결과의 발생을 가능케 한 원인들을 탐색하고, 각각의 확인된 원인으로부터 단계적으로 더 근본적인 원인으로 거슬러 올라가는 과정을 반복함으로써 결국에는 잠재적인 시스템취약점에 대해 충분히 세분화된 윤곽을 파악하게 되어 그에 상응한 대응책을 마련할 수 있다는 것이다.

3.1 공격 트리 모델링

슈나이어(Schneier)에 의해 소개된 공격 트리는 다양한 공격에 의거하여 시스템 보안의 특징을 규정짓는 체계적인 방법이며, 공격에 사용되는 모든 가능한 접근 수단을 검토할 수 있게 하여 대응책의 파악과 적용의 최적화를 용이하게 한다.

공격 트리 구성요소는 노드(node), 간선(edge), 커넥터(connector)이다. 각 노드는 공격을 나타내며 루트 노드(root node)는 공격자의 최종 목표이다. 개별 공격 목표인 각 노드는 하위 공격 목표(또는 상위 목표를 달성하는 수단)인 자식 노드로 분해될 수 있다.

간선은 공격의 전이 상태를 표시한다. OR와 AND 커넥터는 2개 이상의 자식 노드들을 가진 노드의 공격 목표 달성을 위한 전제조건으로 자식 노드들 중 1개만 선택 실행이 가능한 경우(OR)와 모든 자식 노드들이 반드시 실행되어야 하는 경우(AND)를 묘사 한다 [8].

슈나이어의 공격 트리를 기본형으로 복잡하고 변형된 공격을 표현하기 위해 커넥터 타입과 노드 속성(attribute) 요소들이 새로 추가되기도 한다. 커넥터 타입으로 예를 들어 우선순위, 시간, 시퀀스(왼쪽에서 오른쪽으로 연속 실행), 또는 문턱값(threshold)을 기반으로 하는 AND 커넥터가 있다. 노드의 속성은 3종류로 분류할 수 있으며, 공격 성취 속성으로 공격의 유효기간, 공격 수준이나 확률, 성공가능성이 있고, 공격 평가 속성으로는 공격에 드는 비용, 시스템에 미치는 영향, 손실 가능성이 있으며, 피해 시스템의 속성으로는 시스템 취약성, 네트워크/시스템 구성, 액세스 권한 등이 있다 [10][12]. 그 밖에 간선 확장(edge augmentation)이 있으며, 이를 이용하여 간선에 공격 행위를 명시하고 공격 행위에 대한 시그니처(signature)를 추출하여 공격과 관련된 로그만을 필터링할 수 있다 [9].

3.2 사이버 보안 위험 평가

시스템의 잠재적 보안 취약성을 조사하기 위해서는 취약성에 대한 위험을 평가하고 등급을 나누는 방법이 필요하다. 이를 위해 시스템 상태와 보안 환경을 고려하여 위험에 영향을 미치는 지표를 결정한다.

결정된 지표를 기준으로 먼저 공격 트리의 각 leaf node(최하위의 자식 없는 노드)에 지표 값이 부여된다. 공격 트리 내부 노드(leaf node를 제외한 모든 다른 노드)의 값은 그의 자식 노드의 값으로부터 산정된다. 이때 커넥터가 AND이면 자식 노드들 중의 최대값이, OR이면 자식 노드들 중의 최소값이 주어진다.

분석의 최종 목표는 루트 노드와 연관된 지표 값을 결정하고 이 값에 영향을 미치는 공격 경로를 이해하는 것이다. 즉, 루트 노드의 지표 값은 시스템을 손상시키는데 필요한 수단이 무엇이며, 발생 가능성이 가장 큰 공격 방법과 어디에 보안 대책이 필요한지를 나타낸다. 다음은 위험 지표가 될 수 있는 요소들과 '기술 난이도'를 지표로 선택했을 때의 등급 분류 예이다 [11].

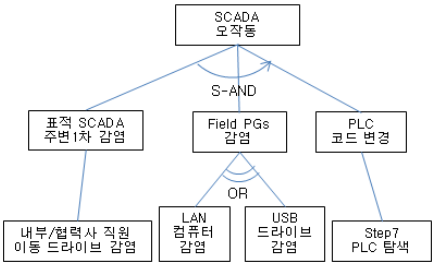
- 위험 지표
  - 기술 난이도
  - 체포 가능성
  - 공격 비용
  - 공격 성공 가능성
  - 사이트 상태
  - 대응 수단의 설치 여부

- '기술 난이도'에 따른 1-4까지의 등급 값
  - 쉬움(1): 숙련 기술이 거의 필요 없음
  - 보통(2): 평균 사이버 해킹 기술
  - 어려움(3): 높은 수준의 전문 기술
  - 실현 가능성 희박(4): 현재 알려진 최고 해커의 능력을 초과

4. 스턱스넷 공격 트리

앞장에서 설명한 공격 트리 모델의 예로서 잘 알려진 스턱스넷 가상 공격 시나리오를 그림 2와 같이 공격 트리로 구성해 보았다 [4]. 시나리오에 있는 스턱스넷 최신 버전의 개발/완성 과정은 공격 트리에 포함 시키지 않았다. 또한 슈나이어의 트리 모델에 커넥터 S-AND를 추가하였다. S-AND는 시퀀스 AND를 의미하며 왼쪽에서 오른쪽으로 연속 실행하라는 표시이다.

공격의 최종 목표는 지멘스 SCADA 시스템의 오작동을 유도하는 것이다. 우선 공격자는 스턱스넷을 사회 공학적 공격 기법을 통해 표적 주변 내부/협력사 직원의 USB 또는 유지보수용 랩톱에 대한 1차 감염을 수행 한다. 다음은 PLC 프로그래밍에 사용되는 Field PGs를 감염시킬 목적으로 LAN 상의 컴퓨터로 감염을 확산시킨다. 또는 오염된 USB가 PGs에 바로 연결될 수 있다. 끝으로 스텝 7이 실행중인 PLC를 찾아 PLC 코드를 변경시켜 SCADA 오작동을 유도한다.



(그림 2) 스턱스넷 공격 트리

스턱스넷 공격에 이용되었던 취약점들은 주로 이동식 매체의 자동실행, LAN 상의 프린트 스플러 또는 서버 서비스 원격 코드 실행에서 발생하는 취약점이며 현재 모두 패치 되었지만, 스턱스넷의 변종 또는 다른 사이버 공격에 악용될 여지가 많은 SCADA의 잠재적 취약점에 대한 근본적인 대책이 시급하다.

5. 결 론

본 논문은 ICS의 사이버 보안 위협, SCADA 시스템의 구조 및 취약성과 공격 트리 모델링 방법을 이해하는데 많은 도움이 될 것이다. SCADA 시스템의 공격 트리 모델링을 위해서는 전문가적인 관점의 세분화되고 깊이 있는 접근이 필요하다. 다음 연구는 구체적인 대상을 설정하고 그에 대한 공격 트리 분석을 수행하는 것이다. 또한 개발 과정의 초기 단계에 시스템의 보안에 취약한 부분을 인지하고 위험에 미리 대비하기 위해 적용되는 이와 같은 분석 방법을 보안 제품의 벤치마크 테스트 분야에도 적용해 볼 수 있다.

참고문헌

[1] A. Mahboob and J. Zubairi, “Intrusion Avoidance for SCADA Security in Industrial Plants”, IEEE CTS, 2010

[2] Symantec, State of Security Survey, 2011

[3] Symantec, Internet Security Threat Report, Trends for 2010, vol. 16, 2011

[4] Symantec, W32.Stuxnet Dossier Version 1.4, 2011

[5] A. Matrosov, E. Rodionov, D. Harley and J. Malcho, Stuxnet Under the Microscope revision 1.31, eset, 2006

[6] K. Stouffer, J. Falco and K. Scarfone, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, NIST. Spec. Publ. 800-82, 164pages, 2006

[7] P. Welander, “10 Control System Security Threats,” Control Engineering, 2007.

[8] B. Schneier, “Attack Trees", Dr. Dobb's Journal, 24(12):21-29, 1999

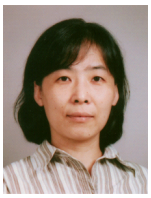
[9] J.Wang, R-W. Phan, J. Whitley and D. Parish, " Augmented Attack Tree Modeling of Distributed Denial of Services and Tree Based Attack Detection Method", In Proceedings of IEEE 10th International Conference on CIT, 2010

[10] J.Wang, R-W. Phan, J. Whitley and D. Parish, " Unified Parametrizable Attack Tree", International Journal for ISR, vol. 1, 2011

[11] E. Byres, "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems", International Infrastructure Suvivability Workshop, Lisbon, 2004

[12] P. Khand, "System Level Security Modeling Using Attack Trees", Proceedings of the 2nd International Conference on Computer Control and Communication, 2009

[저 자 소 개]



김 경 아 (Kyung-Ah Kim)

1999년 Univ. of Marburg
컴퓨터 과학 학사
2003년 Univ. of Marburg
컴퓨터 과학 석사
현재 경기대학교
산업보안 박사과정

email : aokkah@nate.com

김 귀 남 (Kui-nam Kim)

1989 Univ. of Kansas 수학과 학사
1993 Colorado State Univ
통계학과 석사
1994 Colorado State Univ
산업공학과 박사

email : harap123@hanmail.net

이 대 성 (Dae-sung Lee)

1999년 2월 인하대학교
전자계산공학과 학사
2001년 2월 인하대학교
전자계산공학과 석사
2008년 2월 인하대학교
정보공학과 박사

email : xdillema@naver.com